UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,208	03/01/2004	Bruce E. Johnson	MS1-1910US	1947

22801 7590 04/08/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
04/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,208	JOHNSON ET AL.	
	Examiner	Art Unit	
	Amare Tabor	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15-19,21-28 and 30-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-19,21-28 and 30-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Correspondence in response to Amendments and REMARKS filed on January 18, 2008.

2. Claims 1-11, 13, 19, 21, 27, 28, 31 and 34 are amended, Claims 14, 20 and 29 are cancelled.

3. Claims 1-13, 15-19, 21-28 and 30-36 are pending.

Response to Arguments

4. Applicant's arguments with respect to the pending Claims have been considered but are moot in view of the new ground(s) of rejection.

Specification

5. The disclosure is objected to because of the following informalities: In response to the first non-final office action, Applicants have amended the specification by deleting non-statutory subject matter(s) from par.[0025]. However, par.[0040] should also be amended for the same reasons; i.e., the paragraph defines “computer-readable medium” including “carrier waves” and/or “signals”, which are not statutory.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-13, 15-19 and 30-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over “McManis” (US 5,970,145) in view of Abadi et al. (US 7,203,833 B1), referred as “Abadi” hereinafter.

As per Claim 1, McManis teaches,

A computer readable medium [see FIG.1-3B; and for example, Claims 7-10], comprising instructions for metering execution of code [see for example, col.1, lines 8-11, "*The present invention relates to systems and methods for* ***restricting the use of executable modules*** *such that each executable module can be dynamically linked only to other executable modules whose authenticity has been verified*"], the instructions comprising: receiving, at a protected service, a call from an application requesting asking for execution of the protected service within a first runtime area [see **Begin Execution of Proc A 200** in FIG.2; and for example, col.3, lines 61–67, "*Referring to FIGS. 2 and 3, an executable procedure (e.g., the "main application A procedure" 128-A in FIG. 1) in program* ***module A begins execution*** *(step 200). For the purposes of this discussion, the procedure in program module A that is being executed will be called "procedure A" and the procedure that it is attempting to call in program module B will be called "procedure B"*"];

requesting permission for the execution [see **Req. Verification of B 202-Verification of B 204** and **Req. Verification of A 222-Verification of A 230** in FIG.2; and for example, col.4, line 1-4, "*Prior to making a procedure call to an executable procedure in program module B (step 220),* ***procedure A makes a procedure call to the verifier*** *to request verification of the authenticity of program module B (step 202)*"], wherein the request is made by the protected service to a metering engine [see **Verifier** in FIG.2] operating in a second runtime area [see for example, col.4, lines 4-8, "*The verifier then attempts to verify the authenticity of program module B and sends a return value to procedure A to indicate whether or not* ***the verification of program module B*** *was successful (step 204)*"], wherein the request is made through a secure transmission layer [see steps **202-204** and **222-230** in FIG.3A-3B; and for example, col. 3, line 9-16, "*More specifically,* ***the verifier****, which is preferably* ***a distinct trusted object*** *(or alternately* ***a trusted system service procedure****) receives the request message from procedure A (step 206), …*"];

and, analyzing the request, at the metering engine, wherein the analyzing comprises: referencing, within the metering engine [see **Verifier: Verify Authenticity of Program Module B 204** and **Verifier: 230** in FIG.3A-3B], a service contract comprising rules governing operation of the protected service [see steps

206-212; and for example, col.4, line 9-52, "*More specifically, the verifier, … **receives the request message from procedure A (step 206)**, and **decodes** (step 208) a digital signature embedded in program module B using a public key provided by the calling procedure (i.e., procedure A). … program module A……MD.sub.B =HashFunction(Program Module B)… Digital Signature.sub.B =Encrypt(MD.sub.B +HashFunction ID, PrivateKey)+ClearText ID of Program Module B's Source…digital signature with the public key to generate a signature based message digest DS-MD.sub.B, and a hash function ID… DS-MD.sub.B +HashFunction ID=Decode (Digital Signature.sub.B -ClearText ID, PublicKey)……..**verifier then compares the computed message** digest MD.sub.B with the message digest DS-MD.sub.B in the …*". See also 232-238 in FIG.3A-3B; and for example, col.5, lines 27-62].

McManis teaches using metering engine and rules to decide the requested permission [see **Verifier** in FIG.2; and steps 206-212/232-238 in FIG.3A-3B], but fails to disclose referencing a secure store of meter data, wherein the meter data comprises historical data reflecting past operation of the protected service; using the meter data to decide the requested decision and updating the metering data to reflect the analysis.

However, in the same field of endeavor, Abadi discloses referencing secure store of meter data [see FIG.2], wherein the meter data comprises historical data reflecting past operation of the protected service [see step **206 STORE CURRENT RIGHTS…**]; using the meter data to decide the requested decision [see step **207 USE CURRENT RIGHTS TO TAKE SECURITY DECISIONS…**] and updating the metering data to reflect the analysis [see step **208 UPDATE CURRENT RIGHTS…**].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to combine McManis and Abadi because both inventions are in the fields of protecting software-codes from running in unauthorized systems. One having ordinary skill in the art would be motivated to modify the system of McManis by incorporating the secure store meter data teaching of Abadi to enhance the security of the software. The modification ensures that double-security mechanism is implemented before executing the software by checking previous activities performed on the software [see **abstract;** and col.2, line 66 to col.3, line 25 of Abadi].

As per Claim 11, McManis teaches,

A processor-readable medium comprising processor-executable instructions for metering execution of code [see for example, col.1, lines 8-11], the processor-executable instructions comprising instructions for [see FIG.1-3B; and for example, Claims 7-10]: receiving, at a protected service, a call from an application asking for execution of the protected service [see **Begin Execution of Proc A 200** in FIG.2; and for example, col.3, lines 61–67];

requesting authorization to execute the protected service [see **Req. Verification of B 202-Verification of B 204** and **Req. Verification of A 222-Verification of A 230** in FIG.2; and for example, col.4, line 1-8], wherein the authorization request is made from the protected service to a metering engine through a secure transmission layer [see steps **202-204** and **222-230** in FIG.3A-3B; and for example, col. 3, line 9-16]; and

analyzing, with the metering engine, a contract in view of meter data to determine if the authorization request to use the protected service by the application should be allowed [see **Verification Denied** and **Verified** in FIG.3A-3B], and wherein the analyzing comprises: referencing, within the metering engine, the contract, wherein the contract comprises rules governing operation of the protected service [see **Verifier: Verify Authenticity of Program Module B 204** and **Verifier: 230** in FIG.3A-3B], a service contract comprising rules governing operation of the protected service [see steps 206-212; and for example, col.4, line 9-52. See also 232-238 in FIG.3A-3B; and for example, col.5, lines 27-62].

McManis teaches metering engine and using the rules to decide the requested authorization [see **Verifier** in FIG.2; and steps 206-212/232-238 in FIG.3A-3B], but fails to disclose referencing a secure store of meter data wherein the meter data comprises historical data reflecting past operation of the protected service; using the meter data and updating the metering data to reflect the analysis.

However, in the same field of endeavor, Abadi discloses using and referencing secure store of meter data [see FIG.2], wherein the meter data comprises historical data reflecting past operation of the protected service [see step **206 STORE CURRENT RIGHTS…**]; using the meter data to decide the requested decision [see step **207 USE CURRENT RIGHTS TO TAKE SECURITY DECISIONS…**] and updating the metering data to reflect the analysis [see step **208 UPDATE CURRENT RIGHTS…**].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to modify the system of McManis by incorporating the secure store meter data teaching of Abadi to enhance the security of the software. The modification ensures that double-security mechanism is implemented before executing the software by checking previous activities performed on the software [see **abstract;** and col.2, line 66 to col.3, line 25 of Abadi].

As per Claim 19, McManis teaches,

A code-executing device [see FIG.1], comprising: first and second runtime areas with a secure communication channel between them [see **Application Module A 114** and **Application Module B** in FIG.1; and for example, col.3, lines 10-40, "*As shown in FIG. 1, in a preferred embodiment of the invention each application program object instance includes an object header 122, at least … main* ***application A procedure (128-A) in the first program module*** *furthermore includes* ***a procedure call 134 to an executable procedure (e.g., the main application B procedure 128-B) in the second procedure module****. The procedure call 130-A to the program module verifier is* ***logically positioned in the first program module*** *so as to be executed prior to execution of the procedure call 134 to* ***the second program module****…the procedure call 130-B to the program module verifier is logically* ***positioned in the second program module*** *immediately after the entry point to each executable procedure 128-B in* ***the second program module*** *so as to be executed prior to execution of each such procedure 128-B. More generally…*"];

a protected service configured to receive a request from an application for execution of the protected service within the first runtime area [see **Begin Execution of Proc A 200** in FIG.2; and for example, col.3, lines 61–67]; and

a metering engine [see **Verifier** in FIG.2], configured to receive the request and to operate within the second runtime area and to return an allowance code or a rejection code in response to the request by applying rules to meter data [see Verifier either **Deny** or **Verify** Execution of Procedure A in FIG.3A-3B],

wherein the metering engine comprises: an enforcement engine, configured for secure communication with the protected service [*McManis discloses inherent enforcement engine because McManis uses encryption keys to secure communication* - see **Group Public Key(s)/Digital Signature(s) 126-A/124-A, 126-B/124-B, …** in FIG.1; and for example, col.3, lines 41-54, "*In a preferred embodiment of the present invention all the procedures in a designated group, such as all the procedures used by a particular top level application or a suite of top level applications, have the same embedded* ***public key 126 and all are digitally signed using the same private encryption key****, for example using the RSA encryption methodology. However, in an alternate embodiment,* ***different procedures and subgroups of procedures are signed with different private keys****. In the alternate embodiment, the procedure modules that include procedure calls have embedded public keys for verification of the procedures that they can call, and all procedure modules that can be called by other procedures include public keys for verification of the calling procedures*"]; and a service contract, configured to supply the rules governing operation of the protected service, to the enforcement engine [see steps 206-212; and for example, col.4, line 9-52. See also 232-238 in FIG.3A-3B; and for example, col.5, lines 27-62].

McManis teaches enforcement engine [see **Verifier** in FIG.2], but fails to disclose a secure store, within which the meter data is contained, wherein the secure store is configured to supply historical data reflecting past operation of the protected service [see FIG.2].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to modify the system of McManis by incorporating the secure store meter data teaching of Abadi to enhance the security of the software. The modification ensures that double-security mechanism is implemented before executing the software by checking previous activities performed on the software [see **abstract;** and col.2, line 66 to col.3, line 25 of Abadi].

As per Claim 27, McManis teaches,

A computer readable medium comprising instructions for operating a managed code environment [see FIG.1-3B; Claims 7-10; and for example, col.1, lines 8-11], the instructions comprising: an

application configured to consume services from a library of protected services [see **Application Module A 114, B 116, C 118, D 120…** in FIG.1];

a protected service, within the library of protected services, configured to receive a request from the application for execution [see **Begin Execution of Proc A 200** in FIG.2; and for example, col.3, lines 61–67]; and

a metering engine [see **Verifier** in FIG.2], configured to return of an allowance code or a rejection code to the request based on rules governing operation of the protected service [see Verifier either **Deny** or **Verify** Execution of Procedure A in FIG.3A-3B],

wherein the metering engine comprises: an enforcement engine, configured for secure communication with the protected service; and a service contract, configured to supply the rules governing operation of the protected service [*McManis discloses inherent enforcement engine because McManis uses encryption keys to secure communication* - see **Group Public Key(s)/Digital Signature(s) 126-A/124-A, 126-B/124-B, …** in FIG.1; and for example, col.3, lines 41-54], to the enforcement engine [see steps 206-212; and for example, col.4, line 9-52. See also 232-238 in FIG.3A-3B; and for example, col.5, lines 27-62].

McManis teaches enforcement engine [see **Verifier** in FIG.2], but fails to disclose a secure store, within which the meter data is contained, wherein the secure store is configured to supply historical data reflecting past operation of the protected service [see fIG.2].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to modify the system of McManis by incorporating the secure store meter data teaching of Abadi to enhance the security of the software. The modification ensures that double-security mechanism is implemented before executing the software by checking previous activities performed on the software [see **abstract;** and col.2, line 66 to col.3, line 25 of Abadi].

As per Claim 31, McManis teaches,

A code-executing device for metering execution of code see FIG.1-3B; Claims 7-10; and for example, col.1, lines 8-11], the code-executing device comprising: means for calling a protected service from an application [see **Begin Execution of Proc A 200** in FIG.2; and for example, col.3, lines 61–67 – *where McManis discloses inherent means for calling*]; means for calling a metering engine from the protected service [see **Verifier** in FIG.2 – *where McManis discloses inherent means for calling*]; and means for analyzing a contract to determine whether to allow or prohibit use of the protected service by the application [see Verifier either **Deny** or **Verify** Execution of Procedure A in FIG.3A-3B – *where McManis discloses inherent means for analyzing*], and wherein the analyzing comprises: referencing, within the metering engine, a service contract comprising rules governing operation of the protected service [see steps 206-212; and for example, col.4, line 9-52. See also 232-238 in FIG.3A-3B; and for example, col.5, lines 27-62].

McManis teaches using metering engine and rules to decide the requested permission, but fails to disclose referencing a secure store of meter data, wherein the meter data comprises historical data reflecting past operation of the protected service; using the meter data and updating the metering data to reflect the analysis.

However, in the same field of endeavor, Abadi discloses using and referencing secure store of meter data, wherein the meter data comprises historical data reflecting past operation of the protected service; and updating the metering data to reflect the analysis [see FIG.2].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to combine McManis and Abadi because both inventions are in the fields of protecting software-codes running in unauthorized systems. One having ordinary skill in the art would be motivated to modify the system of McManis by incorporating the secure store meter data teaching of Abadi to enhance the security of the software. The modification ensures that double-security mechanism is implemented before executing the software by checking previous activities performed on the software [see **abstract;** and col.2, line 66 to col.3, line 25 of Abadi].

As per Claim 2, McManis teaches,

wherein service contract is selected from among multiple service contracts [see **Verifier Call Instruction 130-A, 130-B, …** in FIG.1].

As per Claims 3 and 4, McManis-Abadi combination teaches,

wherein the first and second runtime areas reside in different partitions of memory [see **Application Module A 114** and **Application Module B** in FIG.1 – *where McManis discloses the runtime areas reside in different partitions is disclosed*]; and wherein the protected service and the metering engine operate within different runtime areas [see abstract and **Verifier** in FIG.1-2 – *where McManis discloses that the verifier could be placed in different runtime area*].

McManis-Abadi fails to disclose wherein the first runtime area is located at a first computing device and the second runtime area is located at a second computing device. However, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention to modify the system of McManis-Abadi by positioning the first and second runtime areas in the respective first and second computing devices to enhance the security of software execution. The modification prohibits an unauthorized execution of the software by implementing a security border between the first and second areas.

Claims 12 and 28 are rejected for the same reasons applied to Claims 3 and 4.

As per Claims 5 and 6, McManis-Abadi combination teaches,

wherein the meter data contains information relevant to more than one protected service [see – FIG.2 and 4A-4D - *where Abadi discloses more than one protective service*]. McManis-Abadi fails to disclose wherein the meter data comprises a number of times a protected service has been called. However, it would have been obvious to modify the system of McManis-Abadi by including the number of times a code has been called into the meter data because this data is an historical data that could be used to check if the security of the code is compromised.

As per Claims 7 and 8, McManis teaches,

wherein requesting permission comprises opening a secure connection between the protected service and a metering engine configured to perform the analysis; and wherein requesting permission comprises sending an encrypted message from the protected service in the first runtime area to the metering engine within the second runtime area [see **Group Public Key(s)/Digital Signature(s) 126-A/124-A, 126-B/124-B, …** in FIG.1].

Claim 18 is rejected for the same reasons applied to the rejection of Claims 7 and 8.

As per Claims 9 and 10, McManis teaches,

wherein the permission was given, additionally comprising: executing the protected service; and returning results of the execution to the application [see **Complete execution of Procedure A 254** in FIG.3B]; and, wherein the permission was not given, additionally comprising returning notice of failure to execute the protected service to an application that initiated the call [see **Procedure A throws exception and aborts 218** in FIG.3A].

Claims 16-17 and 32-33 are rejected for the same reasons applied to the rejection of Claims 9 and 10.

As per Claim 13, McManis-Abadi combination teaches,

wherein the analyzing comprises instructions for: analyzing the contract using the meter data [see FIG. 2 and 4A-4B of Abadi] and identity of the protected service as input to the analysis [see **Object Class Header 122-A, 122-B,…** in of FIG.1 of McManis].

As per Claim 15, McManis-Abadi combination teaches,

wherein the metering of code execution is performed in a managed code environment [see of **abstract** of McManis and FIG.4B-4B of Abadi – *where McManis and Abadi discloses managed code environment*].

Claims 23 and 36 are rejected for the same reasons applied to the rejection of Claim 15.

As per Claim 21, McManis-Abadi combination teaches,

wherein the metering engine is configured to: use identity of the protected service [see **Object Class Header 122-A, 122-B,…** in of FIG.1 of McManis] and data from the secure store of meter data as input to an analysis [see FIG.2 and 4A-4B of Abadi] providing return of the allowance code or the rejection code [see **Procedure A throws exception and aborts 218** in FIG.3A and **Complete execution of Procedure A 254** in FIG.3B of McManis]; and update the secure store of meter data to reflect the analysis [see FIG.2 and 4A-4B of Abadi].

Claim 30 is rejected for the same reasons applied to the rejection of Claim 21.

As per Claim 22, McManis-Abadi combination teaches,

wherein the code-executing device is a cellular telephone [see Computer **100** in FIG.1 of McManis– *where McManis disclose any kind of computer can be used for implementation.* See also **Computing Environment 100** in FIG.1 of Abadi; and for example, col.4, lines 22-43, "*FIG. 1 illustrates an example of a suitable computing system environment 100 in which the invention may be implemented. The computing system environment 100 is only one example …numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, … include…* ***personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, disk controllers, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers****, distributed computing environments that include any of the above systems or devices, and the like*"].

As per Claim 24, McManis-Abadi combination teaches,

wherein the code-executing device is a compound device [see FIG.1], and wherein the protected service is contained on a first portion of the compound device and the metering engine is contained on a second portion of the compound device [see abstract and FIG.1-2 – *where McManis* ***Application Module A*** *and* ***Verifier*** *could be contained in the first and second areas*]

McManis-Abadi fails to disclose wherein the first portion of the compound device is remotely located from the second portion of the compound device. However, it would have been obvious to remotely locate the first portion of the combined device in order to secure the device from physical tampering by unauthorized users.

As per Claims 25 and 26, McManis teaches,

additionally comprising a library of protected services, within which the protected service is contained; and additionally comprising a library of applications, within which the application is contained [see **Application Module A 114, B 116, C 118, D 120…**].

As per Claim 34, McManis-Abadi combination teaches,

wherein the means for analyzing the contract comprises: means for analyzing the contract using identity of the application [see **Application Module A, B, C, D, …** in FIG.1 of McManis], identity of the protected service [see **Object Class Header 122-A, 122-B,…** in of FIG.1 of McManis], rules within the contract [see steps 206-212 and 232-238 in FIG.3A-3B], and data from a secure store of meter data as input to the analysis [see FIG.2 of Abadi].

As per Claim 35, McManis teaches,

wherein the means for calling the metering engine comprises: means for opening a secure connection between the protected service and the metering engine [see **Group Public Key(s)/Digital Signature(s) 126-A/124-A, 126-B/124-B, …** in FIG.1 – *where McManis discloses inherent means for opening secure connection is disclosed*]; and means for operating the protected service and the metering engine within distinct runtime areas [see FIG.1-2 – *where McManis discloses inherent means to operate the verifier and procedure A within distinct runtime areas*].

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

Amare Tabor
(AU 2139)